From: MEGE, Alexandre <alexandre.mege@airbus.com>
Sent: Monday, June 10, 2019 12:45 PM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: LAEM

Dear all,

It seems the reference implementation of LAEM does not handle messages with empty PlainText.

It is visible in the submitted KAT, where messages with empty PT generate empty tags at output.

Ex: laemsimon128v1

Count = 1

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 000102030405060708090A0B0C0D0E0F

PT =

AD =

CT =

Count = 2

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 000102030405060708090A0B0C0D0E0F

PT =

AD = 00

CT =

Count = 3

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 000102030405060708090A0B0C0D0E0F

PT =

AD = 0001

CT =

Best regards,

Alexandre Mège

This document, technology or software does not contain French national dual-use or military controlled data nor US national dual-use or military controlled data